

[Anmerkung Bearbeiter: Namen und Firmen, Rechtsformen und Produktbezeichnungen, Adressen (inkl. URLs, IP- und E-Mail-Adressen), Aktenzahlen (und dergleichen), etc., sowie deren Initialen und Abkürzungen können aus Pseudonymisierungsgründen abgekürzt und/oder verändert sein. Offenkundige Rechtschreib-, Grammatik- und Satzzeichenfehler wurden korrigiert.]

## B E S C H E I D

## S P R U C H

Die Datenschutzbehörde entscheidet über die Datenschutzbeschwerde von Dr. Ida A\*\*\* (Beschwerdeführerin) vom 23. Juni 2018 gegen 1) das Bundesministerium für Europa, Integration und Äußeres (Erstbeschwerdegegner) und 2) das Bundeskanzleramt (Zweitbeschwerdegegner) wegen Verletzung im Recht auf Geheimhaltung wie folgt:

- Die Beschwerde wird abgewiesen.

Rechtsgrundlagen: §§ 1 Abs. 1 und 2, 24 Abs. 1 und 5 des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999 idgF; Art. 4 Z 5, Art. 25 und 32 der Datenschutz-Grundverordnung (DSGVO), ABl. Nr. L 119 vom 4.5.2016, S. 1.

## B E G R Ü N D U N G

### A. Vorbringen der Parteien und Verfahrensgang

1. Die Beschwerdeführerin brachte am 23. Juni 2018 zwei - beinahe inhaltsgleiche - Beschwerden gegen den Erst- und Zweitbeschwerdegegner ein und behauptete darin eine Verletzung im Grundrecht auf Datenschutz wegen unterlassener Datenlöschung bzw. Pseudonymisierung. Die Beschwerdeführerin brachte zusammengefasst vor, dass die Beschwerdegegner sensible persönliche Daten der Beschwerdeführerin in elektronischer Form und ohne Pseudonymisierung speichern würden. Konkret würden die Daten Informationen zum Sexualleben und zur Gesundheit der betreffen. Der Staat habe sich diese Daten im Jahre 2007 bei einer rechtswidrigen verdeckten Ermittlung beschafft. Diesbezüglich wären bereits mehrfach Verfahren vor der Datenschutzbehörde bzw. der ehemaligen Datenschutzkommission anhängig gemacht worden. Weitere Daten (damit wohl gemeint: die weitere Speicherung von Daten) wären das Ergebnis von nachfolgenden Verfahren insbesondere zur Wahrung ihrer Rechte. Die Beschwerdegegner hätten ihre Daten im Jahre 2014 im Zusammenhang mit einer internationalen Beschwerde erhalten („X gegen Österreich, UNO Dokument

CEDAW/C/\*\*3/D/1\*/2014 vom 11. Juli .2016“), die sich auch gegen die Datenbeschaffung gerichtet habe und die seither in Wien und Genf in elektronischer Form archiviert wären. Die Beschwerdegegnerin habe bereits am 24. Juli 2016 ein Ersuchen um Datenlöschung an den Erstbeschwerdegegner bzw. ein Ersuchen um Skartierung der Papierakten an den Zweitbeschwerdegegner gestellt, dem jedoch jeweils nicht entsprochen worden wäre, da die Archivierung besagter Daten zur Dokumentation verschiedener innerstaatlicher Verfahren gesetzlich vorgesehen und auch zur Dokumentation des besagten internationalen Beschwerdeverfahrens nötig sei. Das BVwG habe bereits eine entsprechende Beschwerde gegen diese unterlassene Datenlöschung ua mit der Begründung abgewiesen, dass eine Datenlöschung unmittelbar nach dem Abschluss eines Verfahrens nicht mit rechtsstaatlichen Prinzipien vereinbar sei (Verweis auf BVwG vom 31. August 2017, Zl. W214 2152086).

Die Beschwerdeführerin habe nunmehr zwei Jahre nach Abschluss des besagten Verfahrens mit E-Mail vom 25. Mai 2018 die Beschwerdegegner um Löschung ihrer personenbezogenen Daten ersucht, die entsprechenden Löschbegehren liegen dem Akt als Kopie bei. Sie führte weiter aus, dass das Löschbegehren für sie auch dann erfüllt wäre, wenn eine Pseudonymisierung durchgeführt werden würde. Die unterlassene Pseudonymisierung sei eine Verletzung des Grundrechts auf Datenschutz. Es wäre unverhältnismäßig, wenn Daten in einer nicht pseudonymisierten Form aufbewahrt würden. Die Beschwerdeführerin befürchte, dass ihre Identität in den folgenden Jahrzehnten bei jedem Zugriff auf die Daten offengelegt werde, was nicht mehr mit dem öffentlichen Interesse begründet werden könne. Insbesondere wären ihre Daten bei einem erfolgreichen Hacker-Angriff auf die Server der Beschwerdegegner sofort öffentlich zugänglich. Wenn Daten aufbewahrt werden würden, um „österreichische Rechtsansprüche“ gegen die Neueinbringung einer gleichartigen Beschwerde durch sie bei einem anderen Tribunal zu verteidigen, dann werde der Dokumentationszweck durch die geforderte Pseudonymisierung nicht beschränkt. Nach Rechtsansicht des VfGH müsse für die fortgesetzte Aufbewahrung sensibler persönlicher Daten eine aktuelle und konkrete Notwendigkeit geltend gemacht werden (Verweis auf VfGH vom 12.12.2018, Zl. E3249/2016). Auch aus der DSGVO wäre abzuleiten, dass weitgehende Datenschutzmaßnahmen der Regelfall für die Archivierung sein müssten. So normiere Art. 5 Abs. 1 lit c DSGVO das Prinzip der Datenminimierung und als Instrument dazu führe Art. 25 Abs. 1 DSGVO die Pseudonymisierung an. Die Unterlassung dieser oder vergleichbarer Schutzmaßnahmen wäre ein mit dem Grundrecht auf Datenschutz unvereinbarer leichtfertiger Umgang mit sensiblen Daten.

2. Mit Stellungnahme vom 25. Juni 2018 übermittelte die Beschwerdeführerin die Antwortschreiben der Beschwerdegegner, die dem Löschbegehren der Beschwerdeführerin vom 25. Mai 2018 jeweils nicht entsprochen haben.

3. Mit Mangelhebungsauftrag vom 3. Juli 2018 forderte die Datenschutzbehörde die Beschwerdeführerin auf, ihre Beschwerde entsprechend den gesetzlichen Vorschriften zu präzisieren und konkret darzulegen, in welchen Rechten sich die Beschwerdeführerin als verletzt erachtet.

4. Die Beschwerdeführerin brachte dazu mit Schreiben vom 7. Juli 2018 vor, dass Verfahrensgegenstand die Frage der Rechtswidrigkeit der Datenspeicherung ohne Pseudonymisierung sei. Es ginge der Beschwerdeführerin darum, dass ihr Name und andere, zur Identifizierung geeignete Informationen von den sonstigen Daten so abgetrennt würden, dass aus den verbleibenden Daten alleine nicht mehr auf ihre Identität geschlossen werden könne. Indem die Beschwerdegegner die Datenlöschung verweigern und dadurch massiv in das Privatleben der Beschwerdeführerin eingreifen würden, unterlägen sie der Verpflichtung, die durch die Datenspeicherung entstehenden Risiken zu minimieren, wozu die Pseudonymisierung, oder eine gleichwertige technische Maßnahme zähle.

5. Der Erstbeschwerdegegner führte mit Stellungnahme vom 7. August 2018 zusammengefasst aus, dass das BVwG mit dem seitens der Beschwerdeführerin zitierten Erkenntnis vom 31. August 2017, Zl. W214 2152086-1, auch ins Treffen geführt habe, dass ein öffentliches Dokumentationsinteresse einer Löschung entgegenstehe. Die Argumentation des BVwG hinsichtlich dieses Dokumentationsinteresses würde auch mit der neuen Rechtslage gemäß Art. 5 Abs. 2 lit. e DSGVO iVm § 2 Z 3 und § 5 des Bundesarchivgesetzes und Z 9 der Anlage zu § 2 Abs. 1 der Bundesarchivgutverordnung sowie § 25 Denkmalschutzgesetz weiter anwendbar bleiben. Demnach handle es sich bei Schriftgut von Verfahren vor dem Verfassungsgerichtshof, dem Verwaltungsgerichtshof und vor internationalen Institutionen um Archivgut, das nach dem Denkmalschutzgesetz unter Schutz stehe. Im vorliegenden Fall wäre nicht nur eine internationale Institution befasst (CEDAW), sondern auch beim VwGH eine – noch anhängige – außerordentliche Revision eingebracht. Laut § 5 Abs. 3 Bundesarchivgesetz sei dieses Schriftgut zur Archivierung unter Verschluss dem Österreichischen Staatsarchiv zu übergeben. Bis zur Übernahme des Schriftgutes wären die übergebenden Bundesdienststellen und ab der Übernahme das Österreichische Staatsarchiv Verantwortliche iSv Art. 4 Z 7 DSGVO.

Hinsichtlich der Prüfung der Möglichkeit der Pseudonymisierung der die Beschwerdeführerin betreffenden Akte wurde ausgeführt, dass die Akten, welche Daten

der Beschwerdeführerin enthielten, als Verschlussakten geführt würden, wobei die strengste Verschlussstufe „Verschluss sensibel“ verwendet werde. Die Akten wären im elektronischen Akt (ELAK) mit dieser Sicherheitsstufe markiert und mit den entsprechenden Zugriffsrechten versehen. Zugriff auf den Inhalt dieser Akten hätten somit ausschließlich die im Aktenlauf namentlich vorgeschriebenen Bediensteten, Personen mit Leiterrolle in den vorgeschriebenen übergeordneten Organisationseinheiten und LeiterInnen der im Workflow beteiligten Gruppen sowie Revisoren. Der Großteil der im ELAK geführten Akten wäre im vorliegenden Fall bereits abgelegt, d.h. sie würden sich nicht mehr in Bearbeitung befinden und von berechtigten Personen nur ausnahmsweise und anlassbezogen eingesehen werden. Ein Zugriff erfolge nur durch einen sehr eingeschränkten Personenkreis von Bediensteten, die der Amtsverschwiegenheit unterliegen würden, und lediglich im Zusammenhang mit der gegenständlichen Beschwerde oder etwaigen künftigen Beschwerden der Beschwerdeführerin. Ein derartiger Eingriff in das nach Art. 8 EMRK gewährleistete Grundrecht der Beschwerdeführerin sei als verhältnismäßig einzustufen. Die Einschränkung des Risikos einer ungerechtfertigten Bearbeitung der Daten mittels der erläuterten Einstufung der Akten als „Verschluss sensibel“ biete angesichts der geringen Eingriffswahrscheinlichkeit und intensität somit ein dem Risiko angemessenes Schutzniveau gemäß Art. 32 Abs. 1 DSGVO. Eine Pseudonymisierung als zusätzliche Schutzmaßnahme werde aufgrund des gesetzlich vorgegebenen und gerichtlich bestätigten Dokumentationsinteresses durch den Erstbeschwerdegegner nicht in Aussicht genommen.

6. Der Zweitbeschwerdegegner brachte dazu mit Stellungnahme vom 31. Juli 2018 zusammengefasst vor, dass auf eine Pseudonymisierung kein Rechtsanspruch bestehe, da im Sinne von Art. 25 DSGVO eine Interessenabwägung bzw. eine Abwägung verschiedener Faktoren, wie insbesondere Art und Umfang der Verarbeitung, Risikopotential, Angemessenheit der Kosten und Stand der Technik vorgenommen werden müsse, um die Maßnahmen zu definieren, die die geeignetste Datensicherheitsmaßnahme seien. Eine Pseudonymisierung könne im gegenständlichen Fall unter anderem deshalb nicht zur Anwendung kommen, weil der Sachverhalt, der sich aus einer Vielzahl von unstrukturierten Daten zusammensetze (Stellungnahmen, Berichte, Aktenvermerke und dergleichen) bzw. der gesamte umfangreiche Akt lesbar bleiben müsse, was nach einer Pseudonymisierung nicht mehr gewährleistet wäre. Allein aus diesem Grund sei die Pseudonymisierung, abgesehen von dem enormen Aufwand, der erforderlich wäre, keine geeignete Maßnahme. Insbesondere, da durch eine Pseudonymisierung keine Erhöhung des Schutzniveaus gegenüber dem derzeit ohnehin schon sehr hohen Schutzniveau erfolgen würde und selbst bei Pseudonymisierung die Auflösungen unter Verschluss aufzubewahren wären. Einige Faktoren, die zu dem

derzeitigen sehr hohen Schutzniveau beitragen würden, wären das Vorhandensein eines strikten Berechtigungskonzepts, die Amtsverschwiegenheit der MitarbeiterInnen, eine Ende-zu-Ende Verschlüsselung (Client-Server) mit starkem Verschlüsselungsalgorithmus sowie der Betrieb durch die Bundesrechenzentrum GmbH als Auftragsverarbeiter, die über mehrere Zertifizierungen im Zusammenhang mit IT-Sicherheit verfüge.

7. Die Datenschutzbehörde teilte mit Schreiben vom 9. August 2018 allen Parteien mit, dass die Beschwerde gegen den Erstbeschwerdegegner sowie die Beschwerde gegen den Zweitbeschwerdegegner aufgrund desselben Sachverhalts gemäß § 39 Abs. 2 AVG zur gemeinsamen Entscheidung unter der GZ: DSB-D123.070 verbunden wurde.

8. Die Beschwerdeführerin replizierte darauf - nach Parteiengehör zu den Ergebnissen des Ermittlungsverfahrens - in ihrer Stellungnahme vom 10. August 2018 zusammengefasst, dass sie sich zur Rechtsgrundlage für die Pseudonymisierung auf Art. 5 Abs. 1 lit c stütze. Es sei eine Abwägung iSv Art. 8 EMRK erforderlich, wie die im öffentlichen Interesse erfolgende Archivierung ihrer Daten derart gestaltet werden könne, dass der damit verbundene Eingriff auf ihr Grundrecht auf Datenschutz am gelindesten erfolge. Die Pseudonymisierung könne bei dieser Abwägung nicht ignoriert werden. Die Beschwerdeführerin bestreite zwar nicht, dass aufgrund der bereits getroffenen Maßnahmen zur Datensicherung ein hohes Schutzniveau erreicht werden könne, jedoch wären die Beschwerdegegner exponierte Ziele für Angriffe auf die Computersysteme von außen. Im Hinblick auf die beabsichtigte lange Aufbewahrungsdauer der Daten entspreche es jedoch der Lebenserfahrung, dass es in dieser langen Zeit dennoch zu „Datenlecks“ kommen könne. Bereits jetzt absehbare technologische Innovationen könnten die derzeitigen Sicherungsmaßnahmen in den nächsten Jahren obsolet machen. Unabhängig davon würden die getroffenen Maßnahmen nicht unbedingt gegen unzuverlässige Mitarbeiter schützen, auch wenn diesen Mitarbeitern die strafrechtlichen Konsequenzen bewusst wären. Die sie betreffenden Daten wären zwar geschützt, jedoch wäre der Schutz im Vergleich zu den sonstigen elektronischen Akten bei den Beschwerdegegnern nicht besonders höher. Eine Pseudonymisierung wäre auch eine simple Maßnahme, bei der Dokumente weiterhin lesbar wären. Die Beschwerdeführerin erachte sich durch die unterlassene Pseudonymisierung weiterhin im Grundrecht auf Geheimhaltung verletzt.

## B. Beschwerdegegenstand

Einleitend ist auszuführen, dass die Beschwerdeführerin am 25. Mai 2018 ursprünglich ein Löschbegehren an den jeweiligen Beschwerdegegner gestellt und im Rahmen ihrer Eingabe vom 23. Juni 2018 an die Datenschutzbehörde – neben diversen anderen

Rechten (etwa das Recht auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO) – auch eine Verletzung des Rechts auf Löschung gemäß Art. 17 DSGVO geltend gemacht hat. Im weiteren Vorbringen - insbesondere in Beantwortung des Mangelbehebungsauftrags der Datenschutzbehörde vom 7. Juli 2018 - führte die Beschwerdeführerin aber aus, dass Verfahrensgegenstand nunmehr die Frage der Rechtswidrigkeit der Datenspeicherung ohne Pseudonymisierung sei (vgl. zum Begriff der Pseudonymisierung Art. 4 Z 5 DSGVO). Dazu brachte die Beschwerdeführerin bereits in ihrer Eingabe vom 23. Juni 2018, als auch in ihrer Stellungnahme vom 10. August 2018 vor, die „unterlassene Pseudonymisierung“ sei „eine Verletzung des Grundrechts auf Datenschutz“.

Vor diesem Hintergrund waren nicht mehr die erfolglosen Löschbegehren vom 25. Mai 2018 gegen die Beschwerdegegner bzw. eine Verletzung des Rechts auf Löschung gemäß Art. 17 DSGVO zu überprüfen, sondern eine Verletzung von § 1 DS-G.

Aufgrund des Vorbringens der Beschwerdeführerin ergibt sich somit, dass Beschwerdegegenstand nur die Frage ist, ob die Beschwerdegegner die Beschwerdeführerin im Recht auf Geheimhaltung verletzt haben, indem sie die Pseudonymisierung personenbezogener Daten der Beschwerdeführerin in ihren elektronischen Aktensystemen (ELAK) unterlassen haben.

### C. Sachverhaltsfeststellungen

1. Die Beschwerdegegner speichern personenbezogene Daten der Beschwerdeführerin im elektronischen Aktensystem (ELAK).

*Beweiswürdigung: Die getroffenen Feststellungen beruhen auf der insofern unstrittigen Eingabe der Beschwerdeführerin vom 23. Juni 2018 und auf der insofern unstrittigen Stellungnahme des Erstbeschwerdegegners vom 7. August 2018 bzw. des Zweitbeschwerdegegners vom 31. Juli 2018.*

2. Bisher kam es zu keiner Kompromittierung der Datenverarbeitungssysteme der Beschwerdegegner, bei welcher personenbezogene Daten der Beschwerdeführerin offengelegt wurden oder verlustig gingen.

*Beweiswürdigung: Die getroffenen Feststellungen beruhen insofern auf dem Vorbringen der Beschwerdeführerin vom 23. Juni 2018 und 10. August 2018, als sich die Beschwerdeführerin darauf beschränkte, auf einen in Zukunft potenziell eintretenden Schaden hinzuweisen, wie etwa ihr Verweis auf mögliche Hacker-Angriffe, „Datenlecks“, oder absehbare technologische Innovationen, die die derzeitigen Sicherungsmaßnahmen*

*der Beschwerdegegner in den nächsten Jahren obsolet machen könnten. Im vorliegenden Verfahren gibt es auch keine Anhaltspunkte, von einem bereits erlittenen Schaden der Beschwerdeführerin bzw. von einer bereits erfolgten Offenlegung ihrer Daten an unbefugte Dritte auszugehen.*

D. In rechtlicher Hinsicht folgt daraus:

#### 1. Zur Verletzung von § 1 Abs. 1 DSG (Grundrecht auf Geheimhaltung)

Die Beschwerdeführerin hat bis zum Abschluss des vorliegenden Verfahrens keine konkrete Handlung dargetan, durch die sie in ihrem Grundrecht auf Geheimhaltung verletzt worden wäre. Sie beschränkte sich vielmehr darauf, aufgrund einer „unterlassenen Pseudonymisierung“ ihrer Daten im ELAK (noch) nicht manifestierte Ereignisse, wie potenzielle Hacker-Angriffe, „Datenlecks“, oder absehbare technologische Innovationen ins Treffen zu führen, in deren Rahmen die Beschwerdeführerin durch Offenlegung ihrer Daten zukünftig Schaden nehmen könnte.

Die Datenschutzbehörde kann eine Verletzung des Grundrechts auf Geheimhaltung jedoch nur ex post betrachtet feststellen, weshalb die Beschwerde hinsichtlich möglicherweise in Zukunft eintretender Verletzungen bereits aus diesem Grunde abzuweisen war.

#### 2. Zur Geltendmachung spezifischer Datensicherheitsmaßnahmen

Hinsichtlich einer Verletzung des Grundrechts auf Geheimhaltung durch eine „unterlassene Pseudonymisierung“ ist festzuhalten, dass aus der DSGVO kein Recht abzuleiten ist, wonach eine betroffene Person spezifische Datensicherheitsmaßnahmen iSv Art. 32 DSGVO von einem Verantwortlichen verlangen könnte. Ebenso wenig kann eine betroffene Person – wie von der Beschwerdeführerin begehrt – spezifische Maßnahmen zur Datenminimierung iSv Art. 5 Abs. 1 lit. c DSGVO verlangen.

Zwar ist es grundsätzlich möglich, dass eine betroffene Person aufgrund unzureichender Datensicherheitsmaßnahmen eines Verantwortlichen im Grundrecht auf Geheimhaltung verletzt wird (etwa, weil es dadurch zur Offenlegung an unbefugte Dritte kommt), diesfalls müsste jedoch erstens die Verletzung bereits erfolgt sein (vgl. Punkt 1) und zweitens würde der betroffenen Person auch in diesem Fall kein Recht auf Wahl einer spezifischen Datensicherheitsmaßnahme erwachsen.

Wie nämlich aus Art. 32 DSGVO ersichtlich, trifft die Verpflichtung zur Sicherheit der Verarbeitung personenbezogener Daten den Verantwortlichen bzw. den

Auftragsverarbeiter, wobei diese Sicherheit – unter Berücksichtigung der in Abs. 1 dieser Bestimmung genannten Elemente – auf mehrere Arten gewährleistet sein kann.

Auch aus dem Blickwinkel einer systematischen Interpretation der DSGVO kann nicht geschlossen werden, dass der Gesetzgeber einer betroffenen Person ein subjektives Recht auf Einhaltung bestimmter Datensicherheitsmaßnahmen gewähren wollte:

So sind die Rechte betroffener Personen ausdrücklich in Kapitel III angeführt; die Pseudonymisierung findet sich als Maßnahme aber in Kapitel IV, das die objektiven Pflichten von Verantwortlichen und Auftragsverarbeitern regelt.

In diesem Zusammenhang hat bereits die ehemalige Datenschutzkommission festgehalten, dass Datensicherheitsmaßnahmen – auf welche die Beschwerdeführerin offenkundig verweist – lediglich eine Verpflichtung des Verantwortlichen begründen, nicht aber subjektive Rechtsansprüche einer betroffenen Person (vgl. den Bescheid der DSK vom 2. August 2005, GZ: K121.038/0006-DSK/2005). Das Bundesverwaltungsgericht bestätigte diese Ansicht und führte unter Verweis auf die Judikatur der DSK aus, dass die Geltendmachung spezifischer Datenschutzmaßnahmen einer bescheidmäßigen Absprache nicht zugänglich ist (vgl. die Erkenntnisse des BVwG vom 11. Juli 2017, Zl. W214 2117640-1 sowie vom 20. April 2017, Zl. W214 2007810-1).

Diese Verpflichtung des Verantwortliche kann die Datenschutzbehörde nur im Rahmen eines amtswegig eingeleiteten Prüfverfahrens untersuchen (Art. 55 Abs. 1 iVm Art. 57 Abs. 1 lit a und h DSGVO) und den Verantwortlichen gegebenenfalls zur Einhaltung der Verordnung anweisen (Art. 58 Abs. 2 lit d DSGVO). Im vorliegenden Fall liegen jedoch keine Anhaltspunkte vor, die ein entsprechendes amtswegiges Prüfverfahren begründen würden.

### 3. Ergebnis

Im Ergebnis liegt weder eine (bereits erfolgte) Verletzung des Grundrechts auf Geheimhaltung vor, noch kann – wie dargelegt – eine spezifische Datensicherheitsmaßnahme (konkret: Pseudonymisierung) im Rahmen eines Beschwerdeverfahrens geltend gemacht werden.

Vor diesem Hintergrund war spruchgemäß zu entscheiden.